8300 Greensboro Dr.
Suite 1200
McLean, VA 22102

(703) 584-8660
www.fcclaw.com

LNGS | LUKAS, NACE, GUTIERREZ & SACHS, LLP

March 19, 2015

VIA ECFS

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: NOTICE OF EX PARTE PRESENTATION
MB DOCKET NO. 14-90

Dear Ms. Dortch:

On March 17, 2015, Ms. Claudia James of the Podesta Group and the undersigned, both representing the Minority Cellular Partners Coalition ("MCPC"), met with Valery Galasso of Commissioner Rosenworcel's office.

The parties discussed the allegations, set forth in MCPC's letter of March 4, 2015, that AT&T violated § 222(c)(1) of the Communications Act of 1934, as amended ("Act"), and § 1.20003 of the Commission's Rules, when it voluntarily allowed the National Security Agency ("NSA") to have access to telephony and Internet metadata, and telephony and Internet content. Also discussed was AT&T's claim that MCPC's allegations are "outside the scope of the FCC's investigative powers." Letter from Maureen R. Jeffreys to Marlene H. Dortch, MB Docket No. 14-90, at 2 (Mar. 11, 2015) (quoting *AT&T, Inc. and BellSouth Corp.*, 22 FCC Rcd 5662, 5757 (2007)). We also discussed other of the matters set forth in the attached.

Submitted herewith are the handouts that we distributed at the meeting.

This letter is being filed electronically pursuant to § 1.1206 of the rules. Should any questions arise with regard to this matter, please direct them to me.

Very truly yours,

/s/ Thomas Gutierrez

Tom Gutierrez

cc: Valery Galasso, Esq.

MCPC Files Comments in AT&T-DirecTV Merger highlighting AT&T's Misconduct and CALEA Violations as Part of AT&T's Cooperation in NSA Surveillance Programs

- AT&T has engaged in an established pattern of misconduct and bad behavior. Taken together, these actions should bear upon its qualifications to acquire additional FCC licenses in the proposed acquisition of DirecTV.
- In addition to AT&T's many violations over the years, which we do not detail here, MCPC seeks to draw attention to AT&T's repeated violations of CALEA. Pursuant to that law, FCC rules require communications companies to safeguard customers' personal information, ensuring that it is provided to authorities only in accordance with a court-issued warrant or order.
- Both CALEA and its implementing regulations require the FCC to enforce safeguards against the improper sharing of customer information.
- As part of this mandate, AT&T is required to file with the FCC a systems security and integrity (SSI) plan with the commission. This document outlines internal company policies to ensure its own compliance with CALEA. Any employee violation of an SSI constitutes a violation of FCC rules, and carries statutory penalties.
- While requests to review AT&T's SSI plan have been denied, AT&T's widely acknowledged actions in collecting and providing customer data to federal authorities without "appropriate legal authorization" appear to be a direct violation of its SSI plan and of CALEA itself.
- Yet the FCC has not publicly taken any action against AT&T.
- Ironically, in 1998 AT&T urged the FCC to recognize that CALEA requires providers to receive legal authorization "before taking any action to affirmatively implement the interception of communications or access to call-identifying information."
- Only three years later, under the President's Surveillance Program (PSP), AT&T repeatedly and continually agreed to provide the government with covered information before receiving the legal authorization required by CALEA.
- Available evidence indicates that upon receipt of NSA's first request-for-assistance letters, AT&T either blindly implemented them or did not review them carefully.
- Moreover, these letters clearly did not qualify as an appropriate legal authorization under Title III, FISA, CALEA, the Communications Act, or FCC rules, as they could not be considered a court order, a warrant, or a subpoena.
- The first appropriate legal authorization that was presented to AT&T appears to have been the FISC's "Pen Register/Trap & Trace" order that was issued on July 15, 2004.
- AT&T provided the government intercepted telephony and internet communications and access to call-identifying information as part of a dragnet carried on its network for a period of at least 33 months without appropriate legal authorization.
- As has been done with other statutes, the FCC should investigate AT&T's complicity in the PSP to determine whether AT&T engaged in unlawful conduct under CALEA and whether any such violations impact the company's qualifications to obtain DIRECTV's licenses.

THE MINORITY CELLULAR PARTNERS COALITION ("MCPC")

- MCPC filed comments in MB Docket No. 14-90 opposing the merger of AT&T and DIRECTV.
- The members of MCPC were minority partners in the general partnerships that were the initial licensees of the so-called "nonwireline" cellular systems in eleven CMAs.
- AT&T acquired control of the eleven partnerships and used its position as the majority partner to oppress the minority partners, to commit material breaches of the partnership agreements, and to manipulate the finances of the licensee partnerships for its own purposes and profit.
- AT&T "squeezed out" its minority partners by having the assets of the partnerships transferred to newly-formed AT&T affiliates, thereby effectuating the dissolution of the partnerships allegedly under the terms of their partnership agreements.
- AT&T transferred control of eleven the cellular licenses, which it undervalued at $1.6 billion, without prior Commission consent by mischaracterizing the transactions.

ISSUES PRESENTED

- Whether the Commission must reassess AT&T's qualifications in light of its Commission-related misconduct.
- Whether AT&T's acquisition of DIRECTV will substantially reduce competition.
- Whether AT&T violated CALEA and § 222 in its role in the NSA's warrantless domestic surveillance program.

8300 Greensboro Drive
Suite 1200
McLean, VA 22102
www.fcclaw.com
(703) 584-8678

THE COMMISSION'S DUTIES

- To protect the privacy of consumers using the communications infrastructure and to ensure that carriers are protecting consumer information.
- To enforce the § 222 requirement that carriers protect CPNI (*e.g.*, telephone numbers called and received, duration and timing of calls, location of the parties).
- To conduct investigations under § 229 to ensure that carriers comply with their CALEA obligation to require a court order or other lawful authorization to activate interception of communications or access to call-identifying information (dialing or signaling information that identifies the origin, direction, destination, or termination of a subscriber's communication).

CALEA

- "In emergency or exigent circumstances ... a carrier at its discretion may [deliver intercepted communications and call-identifying information, pursuant to a court order or other lawful authorization] by allowing monitoring at its premises if that is the only means of accomplishing the interception or access." 47 U.S.C. § 1002(c).
- "A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission." *Id.* § 1004.
- "The rules prescribed [to implement the requirements of CALEA] shall include rules to implement [27 U.S.C. § 1004] that require common carriers ... to establish appropriate policies and procedures for the supervision and control of its officers and employees ... to require appropriate authorization to activate interception of communications or access to call-identifying information; and ... to prevent any such interception or access without such authorization." *Id.* § 229(b).

8300 Greensboro Drive
Suite 1200
McLean, VA 22102
www.fcclaw.com
(703) 584-8678

AT&T's Systems Security and Integrity ("SSI") Plan

- AT&T was required to appoint a senior officer or employee responsible for ensuring that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization. *See* 47 C.F.R. § 1.20003(a).
- AT&T had to establish policies and procedures – an SSI plan – that would include: (1) a statement that its personnel must receive appropriate legal authorization and appropriate AT&T authorization before enabling law enforcement officials to implement the interception of communications or access to call-identifying information; and (2) an interpretation of the phrase "appropriate authorization" that encompasses the definitions of appropriate legal authorization and appropriate AT&T authorization. *See id.* § 1.20003(b).
- AT&T submitted its SSI plan to the Commission for review in 1999, and is required to submit a plan within 90 days of a merger. *See id.* § 1.20005(a).
- A violation of AT&T's SSI plan is a violation of a rule prescribed by the Commission pursuant to the Communications Act of 1934. *See* 47 U.S.C. § 229(d).

APPROPRIATE LEGAL AUTHORIZATION FOR FOREIGN INTELLIGENCE SURVEILLANCE

- Certification in writing under oath by the Attorney General that the electronic surveillance is solely directed at the acquisition of the contents of communications exclusively between foreign powers and there is no likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party. *See* 50 U.S.C. § 1802(a)(1).
- A Foreign Intelligence Surveillance Court ("FISC") order approving electronic surveillance anywhere within the United States. *See id.* § 1803(a)(1).
- An emergency seven-day authorization issued by the Attorney General. *See id.* § 1805(e).
- A FISC order obtained by the FBI Director requiring AT&T to turn over "any tangible things ... for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." *Id.* § 1861(a)(1).
- A certification in writing by the Attorney General that "no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." *Id.* § 2511(2)(a)(ii)(B).
- A "national security letter" in which the FBI Director (or his designee) certifies that "subscriber information and toll billing records information, or electronic communication transactional records" are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709(b).

AT&T AND THE PRESIDENT'S SURVEILLANCE PROGRAM ("PSP")

- On October 4, 2001, President Bush issued a memorandum ("Authorization") authorizing the NSA to collect telephony and Internet metadata, and telephone and Internet content, for which there was probable cause to believe that one of the communicants was in Afghanistan or was engaged in international terrorism.
- Between the September 11, 2001, attacks and the issuance of the Authorization, AT&T contacted the NSA to offer its help; the NSA made it clear to AT&T that participation in the PSP was voluntary.
- On October 6, 2001, the NSA began to receive telephony and Internet content from AT&T through communications links owned and operated by AT&T.
- In November 2001, AT&T began providing telephony and Internet metadata to the NSA.
- Instead of receiving a certification in writing from the Attorney General that no warrant or court order was required by law and that all statutory requirements had been met, AT&T received 44 request-for-assistance letters from the Director of the NSA between October 16, 2001 and December 14, 2006.
- The NSA's request-for-assistance letters clearly were not appropriate legal authorizations.
- The first appropriate legal authorization that was presented to AT&T was the FISC's "Pen Register/Trap & Trace" order that was issued on July 15, 2004.
- AT&T delivered intercepted telephony and Internet communications, and gave access to call-identifying information concerning substantially all of the communications that were carried on its network, to the NSA for a period of at least 33 months without receiving appropriate legal authorization.

AT&T's Response

- AT&T does not deny that it voluntarily allowed the NSA to intercept communications and have access to CPNI and call-identifying information without appropriate legal authorization.
- Relying on a letter that Chairman Martin wrote to Congress in 2006, AT&T claims that classified nature of the NSA's activities prevents the Commission from investigating the NSA's collection of telephone and Internet metadata, as well as telephone and Internet content.
- The Commission has explicit authority to investigate AT&T's violation of its SSI plan under § 229(c).
- The Commission need not order the production of classified information; it need only review declassified or publicly-disclosed information to determine that AT&T gave the NSA unfettered access to the protected, private telephone records of millions of Americans.
- AT&T does not contend that it obtained appropriate legal authorization (a FISA Court order, a certification under oath by the Attorney General, or a national security letter from the FBI Director) to allow the NSA to intercept communications or to have access to CPNI or call-identifying information.
- The Commission has the duty under §§ 222 and 229 to protect customer privacy and cannot ignore AT&T's egregious violations of the CPNI and CALEA rules.